

3 encoding a plaintext message word M to a ciphertext word C , wherein M corresponds to
4 a number representative of a message and wherein

$$5 \quad 0 \leq M \leq n-1,$$

6 wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \dots \cdot p_k$, k is an integer
7 greater than 2 and p_1, p_2, \dots, p_k are distinct random prime numbers, C is a number
8 representative of an encoded form of message word M , and wherein said encoding step
9 comprises transforming said message word M to said ciphertext word C , whereby

$$10 \quad C \equiv M^e \pmod{n},$$

11 and wherein e is a number relatively prime to $(p_1-1), (p_2-1), \dots$, and (p_k-1) ; and

12 decoding said ciphertext word C to a receive message word M' , said decoding step being
13 performed using a decryption exponent d that is defined by

$$14 \quad d \equiv e^{-1} \pmod{((p_1-1)(p_2-1) \dots (p_k-1))},$$

15 said decoding step including the further steps of,

16 defining a plurality of k sub-tasks in accordance with

$$17 \quad M_1' \equiv C_1^{d_1} \pmod{p_1},$$

$$18 \quad M_2' \equiv C_2^{d_2} \pmod{p_2},$$

19 \vdots

$$20 \quad M_k' \equiv C_k^{d_k} \pmod{p_k},$$

21 wherein

$$22 \quad C_1 \equiv C \pmod{p_1},$$

$$23 \quad C_2 \equiv C \pmod{p_2},$$

24 \vdots

$$25 \quad C_k \equiv C \pmod{p_k},$$

$$26 \quad d_1 \equiv d \pmod{(p_1 - 1)},$$

$$27 \quad d_2 \equiv d \pmod{(p_2 - 1)}, \text{ and}$$

28 \vdots

$$29 \quad d_k \equiv d \pmod{(p_k - 1)},$$

30 solving said sub-tasks to determine results M_1', M_2', \dots, M_k' , and
31

32 combining said results of said sub-tasks to produce said receive message word
33 M' , wherein $M'=M$.

1 22. (Three Times Amended) A cyptographic communications system for establishing
2 communications, comprising:
3 a communication medium;
4 encoding means coupled to said communication medium and adapted for transforming a
5 transmit message word M to a ciphertext word C and for transmitting said ciphertext word C on
6 said medium, wherein M corresponds to a number representative of a message, and
7 $0 \leq M \leq n-1$, wherein n is a composite number of the form,
8 $n = p_1 \cdot p_2 \cdot \dots \cdot p_k$
9 wherein k is an integer greater than 2 and p_1, p_2, \dots, p_k are distinct random prime
10 numbers, and wherein said ciphertext word C corresponds to a number representative of an
11 enciphered form of said message word M and corresponds to
12 $C \equiv M^e \pmod{n}$,
13 wherein e is a number relatively prime to $(p_1-1), (p_2-1), \dots$, and (p_k-1) ; and
14 decoding means communicatively coupled with said communication medium for
15 receiving said ciphertext word C via said medium, said decoding means being operative to
16 perform a decryption process for transforming said ciphertext word C to a receive message word
17 M' , wherein M' corresponds to a number representative of a deciphered form of C , said
18 decryption process using a decryption exponent d that is defined by
19 $d \equiv e^{-1} \pmod{((p_1-1)(p_2-1) \dots (p_k-1))}$,
20 said decryption process including the steps of
21 defining a plurality of k sub-tasks in accordance with
22 $M_1' \equiv C_1^{d_1} \pmod{p_1}$,
23 $M_2' \equiv C_2^{d_2} \pmod{p_2}$,
24 \vdots
25 $M_k' \equiv C_k^{d_k} \pmod{p_k}$,
26 wherein

27 $C_1 \equiv C \pmod{p_1},$

28 $C_2 \equiv C \pmod{p_2},$

29 \vdots

30 $C_k \equiv C \pmod{p_k},$

31

32 $d_1 \equiv d \pmod{(p_1 - 1)},$

33 $d_2 \equiv d \pmod{(p_2 - 1)},$

34 \vdots

35 $d_k \equiv d \pmod{(p_k - 1)},$

36 solving said sub-tasks to determine results M_1', M_2', \dots, M_k' , and

37 combining said results of said sub-tasks to produce said receive message word M'

38 whereby $M' = M$.

1 27. (Three Times Amended) A method for establishing cryptographic communications,

2 comprising the step of:

3 encoding a plaintext message word M to a ciphertext word C , wherein M corresponds to
4 a number representative of a message, and

5 $0 \leq M \leq n-1,$

6 n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \dots \cdot p_k$, wherein k is an integer
7 greater than 2 and p_1, p_2, \dots, p_k are distinct random prime numbers, and wherein the ciphertext
8 word C is a number representative of an encoded form of message word M , wherein said step of
9 encoding includes the steps of

10 defining a plurality of k sub-tasks in accordance with

11 $C_1 \equiv M_1^{e_1} \pmod{p_1},$

12 $C_2 \equiv M_2^{e_2} \pmod{p_2},$

13 \vdots

14 $C_k \equiv M_k^{e_k} \pmod{p_k},$

15 where

$$\begin{aligned}
16 \quad & M_1 \equiv M \pmod{p_1}, \\
17 \quad & M_2 \equiv M \pmod{p_2}, \\
18 \quad & \vdots \\
19 \quad & M_k \equiv M \pmod{p_k}, \\
20 \quad & \\
21 \quad & e_1 \equiv e \pmod{(p_1 - 1)}, \\
22 \quad & e_2 \equiv e \pmod{(p_2 - 1)}, \text{ and} \\
23 \quad & \vdots \\
24 \quad & e_k \equiv e \pmod{(p_k - 1)},
\end{aligned}$$

25 wherein e is a number relatively prime to (p_1-1) , (p_2-1) , ..., and (p_k-1) ,
26 solving said sub-tasks to determine results C_1, C_2, \dots, C_k , and
27 combining said results of said sub-tasks to produce said ciphertext word C .

1 32. (Three Times Amended) A cryptographic communications system for establishing
2 communications, comprising:
3 a communication medium;
4 encoding means coupled to said communication medium and operative to transform a
5 transmit message word M to a ciphertext word C , and to transmit said ciphertext word C on said
6 medium, wherein M corresponds to a number representative of a message, and
7 $0 \leq M \leq n-1$,
8 n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \dots \cdot p_k$ wherein k is an integer
9 greater than 2 and p_1, p_2, \dots, p_k , are distinct random prime numbers, and wherein the ciphertext
10 word C is a number representative of an encoded form of message word M , said encoding means
11 being operative to transform said transmit message word M to said ciphertext word C by
12 performing an encoding process comprising the steps of
13 defining a plurality of k sub-tasks in accordance with

$$\begin{aligned}
14 \quad & C_1 \equiv M_1^{e_1} \pmod{p_1}, \\
15 \quad & C_2 \equiv M_2^{e_2} \pmod{p_2}, \\
16 \quad & \vdots
\end{aligned}$$

17 $C_k \equiv M_k^{e_k} \pmod{p_k},$

18 where

19 $M_1 \equiv M \pmod{p_1},$

20 $M_2 \equiv M \pmod{p_2},$

21 \vdots

22 $M_k \equiv M \pmod{p_k},$

23

24 $e_1 \equiv e \pmod{(p_1 - 1)},$

25 $e_2 \equiv e \pmod{(p_2 - 1)},$ and

26 \vdots

27 $e_k \equiv e \pmod{(p_k - 1)},$

28 wherein e is a number relatively prime to $(p_1 - 1), (p_2 - 1), \dots,$ and $(p_k - 1),$

29 solving said sub-tasks to determine results $C_1, C_2, \dots, C_k,$ and

30 combining said results of said sub-tasks to produce said ciphertext word $C.$

1 37. (Three Times Amended) A method for establishing cryptographic communications,

2 comprising the steps of:

3 decoding a ciphertext word C to a message word M , wherein M corresponds to a number
4 representative of a message and wherein

5 $0 \leq M \leq n-1$

6 wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \dots \cdot p_k$, k is an integer greater
7 than 2 and p_1, p_2, \dots, p_k are distinct random prime numbers, C is a number representative of an
8 encoded form of message word M that is encoded by transforming said message word M to said
9 ciphertext word C whereby

10 $C \equiv M^e \pmod{n},$

11 and wherein e is a number relatively prime to $(p_1 - 1), (p_2 - 1), \dots,$ and $(p_k - 1);$

12 said decoding step being performed using a decryption exponent d that is defined by

13 $d \equiv e^{-1} \pmod{((p_1 - 1)(p_2 - 1) \dots (p_k - 1))},$

14 wherein said step of decoding includes the steps of
15 defining a plurality of k sub-tasks in accordance with

$$16 \quad M_1 \equiv C_1^{d_1} \pmod{p_1},$$

$$17 \quad M_2 \equiv C_2^{d_2} \pmod{p_2},$$

18 \vdots

$$19 \quad M_k \equiv C_k^{d_k} \pmod{p_k},$$

20 wherein

$$21 \quad C_1 \equiv C \pmod{p_1},$$

$$22 \quad C_2 \equiv C \pmod{p_2},$$

23 \vdots

$$24 \quad C_k \equiv C \pmod{p_k},$$

$$25 \quad d_1 \equiv d \pmod{(p_1 - 1)},$$

$$26 \quad d_2 \equiv d \pmod{(p_2 - 1)}, \text{ and}$$

27 \vdots

$$28 \quad d_k \equiv d \pmod{(p_k - 1)},$$

29 solving said sub-tasks to determine results M_1, M_2, \dots, M_k , and
30 combining said results of said sub-tasks to produce said message word M.
31

1 42. (Three Times Amended) A cryptographic communications system for establishing
2 communications, comprising:
3 a communication medium;
4 decoding means communicatively coupled with said communication medium for
5 receiving a ciphertext word C via said medium, and being operative to transform said ciphertext
6 word C to a receive message word M', wherein a message M corresponds to a number
7 representative of a message and wherein,

$$8 \quad 0 \leq M \leq n-1$$

wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \dots \cdot p_k$, k is an integer greater than 2 and p_1, p_2, \dots, p_k are distinct random prime numbers, and wherein said ciphertext word C is a number representative of an encoded form of said message word M that is encoded by transforming M to said ciphertext word C whereby,

$$C \equiv M^e \pmod{n},$$

and wherein e is a number relatively prime to $(p_1-1), (p_2-1), \dots$, and (p_k-1) ;

said decoding means being operative to perform a decryption process using a decryption exponent d that is defined by

$$d \equiv e^{-1} \pmod{((p_1-1)(p_2-1) \dots (p_k-1))},$$

said decryption process including the steps of

defining a plurality of k sub-tasks in accordance with,

$$M_1' \equiv C_1^{d_1} \pmod{p_1},$$

$$M_2' \equiv C_2^{d_2} \pmod{p_2},$$

$$\vdots$$

$$M_k' \equiv C_k^{d_k} \pmod{p_k},$$

wherein,

$$C_1 \equiv C \pmod{p_1},$$

$$C_2 \equiv C \pmod{p_2},$$

$$\vdots$$

$$C_k \equiv C \pmod{p_k},$$

$$d_1 \equiv d \pmod{(p_1 - 1)},$$

$$d_2 \equiv d \pmod{(p_2 - 1)}, \text{ and}$$

$$\vdots$$

$$d_k \equiv d \pmod{(p_k - 1)},$$

solving said sub-tasks to determine results M_1', M_2', \dots, M_k' , and

combining said results of said sub-tasks to produce said receive message word

M' , whereby $M'=M$.

1 47. (Three Times Amended) A method for generating a digital signature, comprising the step
2 of:

3 signing a plaintext message word M to create a signed ciphertext word C, wherein M
4 corresponds to a number representative of a message, and

5 $0 \leq M \leq n-1$,

6 n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \dots \cdot p_k$, wherein k is an integer
7 greater than 2 and p_1, p_2, \dots, p_k are distinct random prime numbers, and wherein the signed
8 ciphertext word C is a number representative of a signed form of message word M, wherein

9 $C \equiv M^d \pmod{n}$, and

10 wherein said step of signing includes the steps of
11 defining a plurality of k sub-tasks in accordance with

12 $C_1 \equiv M_1^{d_1} \pmod{p_1}$,

13 $C_2 \equiv M_2^{d_2} \pmod{p_2}$,

14 \vdots

15 $C_k \equiv M_k^{d_k} \pmod{p_k}$,

16 where

17 $M_1 \equiv M \pmod{p_1}$,

18 $M_2 \equiv M \pmod{p_2}$,

19 \vdots

20 $M_k \equiv M \pmod{p_k}$,

21 $d_1 \equiv d \pmod{(p_1 - 1)}$,

22 $d_2 \equiv d \pmod{(p_2 - 1)}$, and

23 \vdots

24 $d_k \equiv d \pmod{(p_k - 1)}$,

25 wherein d is defined by

26 $d \equiv e^{-1} \pmod{(p_1 - 1) \cdot (p_2 - 1) \cdot \dots \cdot (p_k - 1)}$, and

27 e is a number relatively prime to $(p_1-1), (p_2-1), \dots$, and (p_k-1) ,
28

29 solving said sub-tasks to determine results C_1, C_2, \dots, C_k , and
30 combining said results of said sub-tasks to produce said ciphertext word C.

1 52. (Three Times Amended) A digital signature generation system, comprising:
2 a communication medium;
3 digital signature generating means coupled to said communication medium and operative
4 to transform a transmit message word M to a signed ciphertext word C, and to transmit said
5 signed ciphertext word C on said medium, wherein M corresponds to a number representative of
6 a message, and
7 $0 \leq M \leq n-1$,
8 n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \dots \cdot p_k$ wherein k is an integer
9 greater than 2 and p_1, p_2, \dots, p_k are distinct random prime numbers, and wherein the signed
10 ciphertext word C is a number representative of a signed form of said message word M, wherein
11 $C \equiv M^d \pmod{n}$,
12 said digital signature generating means being operative to transform said transmit
13 message word M to said signed ciphertext word C by performing a digital signature generating
14 process comprising the steps of,
15 defining a plurality of k sub-tasks in accordance with,

$$C_1 \equiv M_1^{d_1} \pmod{p_1},$$

$$C_2 \equiv M_2^{d_2} \pmod{p_2},$$

:

$$C_k \equiv M_k^{d_k} \pmod{p_k},$$

where,

$$M_1 \equiv M \pmod{p_1},$$

$$M_2 \equiv M \pmod{p_2},$$

:

$$M_k \equiv M \pmod{p_k},$$

$$d_1 \equiv d \pmod{(p_1 - 1)},$$

27 $d_2 \equiv d \pmod{(p_2 - 1)}$, and
 28 \vdots
 29 $d_k \equiv d \pmod{(p_k - 1)}$,
 30 wherein d is defined by,
 31 $d \equiv e^{-1} \pmod{(p_1 - 1) \cdot (p_2 - 1) \cdot \dots \cdot (p_k - 1)}$, and
 32 e is a number relatively prime to $(p_1 - 1)$, $(p_2 - 1)$, ..., and $(p_k - 1)$,
 33 solving said sub-tasks to determine results C_1, C_2, \dots, C_k , and
 34 combining said results of said sub-tasks to produce said signed ciphertext word C .

1 57. (Three Times Amended) A digital signature process, comprising the steps of:
 2 signing a plaintext message word M to create a signed ciphertext word C , wherein M
 3 corresponds to a number representative of a message and wherein
 4 $0 \leq M \leq n-1$
 5 wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \dots \cdot p_k$, k is an integer
 6 greater than 2 and p_1, p_2, \dots, p_k are distinct random prime numbers, C is a number
 7 representative of a signed form of message word M , and wherein said encoding step
 8 comprises transforming said message word M to said ciphertext word C whereby,
 9 $C \equiv M^d \pmod{n}$,
 10 wherein d is defined by
 11 $d \equiv e^{-1} \pmod{(p_1 - 1) \cdot (p_2 - 1) \cdot \dots \cdot (p_k - 1)}$, and
 12 e is a number relatively prime to $(p_1 - 1)$, $(p_2 - 1)$, ..., and $(p_k - 1)$; and
 13 verifying said ciphertext word C to a receive message word M' by performing the steps
 14 of,
 15 defining a plurality of k sub-tasks in accordance with
 16 $M_1' \equiv C_1^{e_1} \pmod{p_1}$,
 17 $M_2' \equiv C_2^{e_2} \pmod{p_2}$,
 18 \vdots
 19 $M_k' \equiv C_k^{e_k} \pmod{p_k}$,
 20 wherein

21 $C_1 \equiv C \pmod{p_1},$
 22 $C_2 \equiv C \pmod{p_2},$
 23 \vdots
 24 $C_k \equiv C \pmod{p_k},$
 25
 26 $e_1 \equiv e \pmod{(p_1 - 1)},$
 27 $e_2 \equiv e \pmod{(p_2 - 1)},$ and
 28 \vdots
 29 $e_k \equiv e \pmod{(p_k - 1)},$
 30 solving said sub-tasks to determine results $M_1', M_2', \dots, M_k',$ and
 31 combining said results of said sub-tasks to produce said receive message word
 32 $M',$ whereby $M'=M.$

1 62. (Three Times Amended) A digital signature system, comprising:
 2 a communication medium;
 3 digital signature generating means coupled to said communication medium and adapted
 4 for transforming a message word M to a signed ciphertext word C and for transmitting said
 5 signed ciphertext word C on said medium, wherein M corresponds to a number representative of
 6 a message, and
 7 $0 \leq M \leq n-1,$ wherein n is a composite number of the form
 8 $n = p_1 \cdot p_2 \cdot \dots \cdot p_k,$
 9 wherein k is an integer greater than 2 and p_1, p_2, \dots, p_k are distinct random prime
 10 numbers, and wherein said signed ciphertext word C corresponds to a number representative of a
 11 signed form of said message word M and corresponds to
 12 $C \equiv M^d \pmod{n},$
 13 wherein d is defined by
 14 $d \equiv e^{-1} \pmod{(p_1 - 1) \cdot (p_2 - 1) \cdot \dots \cdot (p_k - 1)},$ and
 15 e is a number relatively prime to $(p_1-1), (p_2-1), \dots,$ and $(p_k-1);$ and

16 digital signature verification means communicatively coupled with said communication
 17 medium for receiving said signed ciphertext word C via said medium, and being operative to
 18 verify said signed ciphertext word C by performing the steps of,
 19 defining a plurality of k sub-tasks in accordance with

$$M_1' \equiv C_1^{e_1} \pmod{p_1},$$

$$M_2' \equiv C_2^{e_2} \pmod{p_2},$$

$$\vdots$$

$$M_k' \equiv C_k^{e_k} \pmod{p_k},$$

24 wherein

$$C_1 \equiv C \pmod{p_1},$$

$$C_2 \equiv C \pmod{p_2},$$

$$\vdots$$

$$C_k \equiv C \pmod{p_k},$$

$$e_1 \equiv e \pmod{(p_1 - 1)},$$

$$e_2 \equiv e \pmod{(p_2 - 1)},$$

$$\vdots$$

$$e_k \equiv e \pmod{(p_k - 1)},$$

34 solving said sub-tasks to determine results M_1', M_2', \dots, M_k' , and

35 combining said results of said sub-tasks to produce said receive message word M'

36 wherein $M'=M$.